PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-259305
(43)Date of publication of application : 13.09.2002

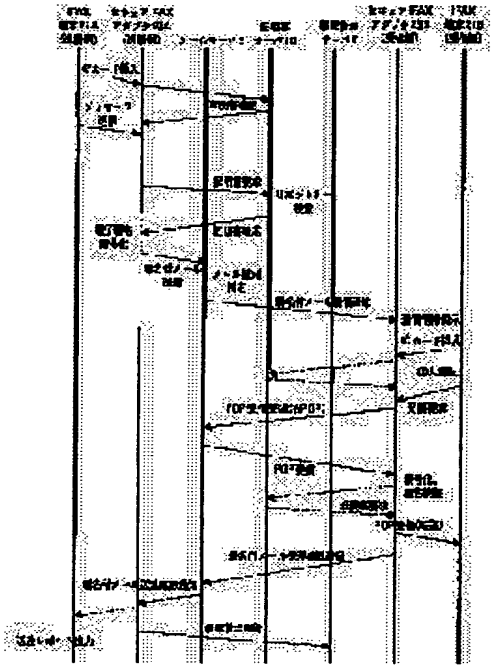
(51)Int.Cl. G06F 13/00
H04L 12/58
H04N 1/00
H04N 1/32
H04N 1/44

(21)Application number : 2001-056607
(22)Date of filing : 01.03.2001

(71)Applicant : MATSUSHITA GRAPHIC COMMUNICATION SYSTEMS INC
(72)Inventor : TOYODA KIYOSHI
MURATA MATSUHISA
AKIMOTO MASAO

(54) CIPHERED MAIL DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a ciphered mail distribution system capable of attaining the conflicting requirements of high secrecy and the urgent distribution of a confidential document.
SOLUTION: When receiving a mail with a signature, a mail server 9 transmits a call income information mail to a secure IFAX adapter 23B on a receiving side to which the receiving person of the mail with the signature is registered. When receiving the call income information mail, the adapter 23B on the receiving side informs the receiving person being the owner of its destination account of the call-incoming of the ciphered mail from the destination account, requests the personal authentication of the receiving person by using an IC card 109 and receives/deciphers the mail with the signature after confirming the receiving person. Thus, the receiving person can fetch the confidential document of the mail with the signature speedily and surely from the server 9.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－259305
（Ｐ２００２－２５９３０５Ａ）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
G06F 13/00	610	G06F 13/00	610 Ｓ	5C062
	640		640	5C075
H04L 12/58	100	H04L 12/58	100 Ｅ	5K030
H04N 1/00	107	H04N 1/00	107 Ｚ	
1/32		1/32	Ｚ	

審査請求　未請求　請求項の数14　ＯＬ　（全15頁）　最終頁に続く

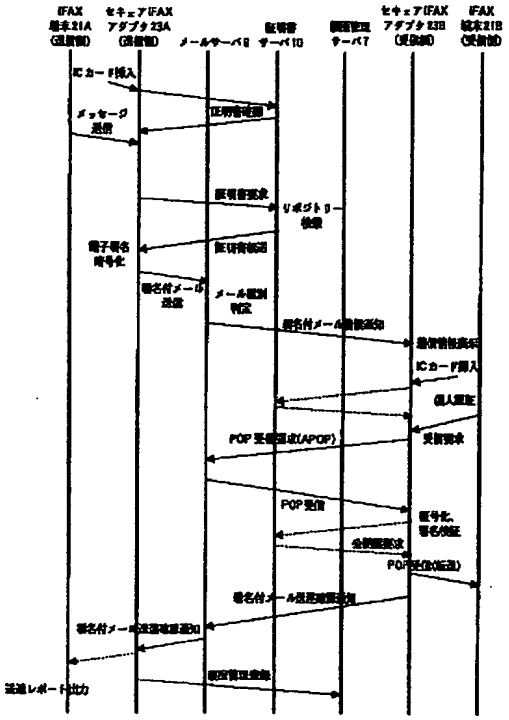
(21)出願番号　特願2001－56607（Ｐ2001－56607）
(22)出願日　平成13年３月１日(2001.3.1)

(71)出願人　000187736
松下電送システム株式会社
東京都目黒区下目黒２丁目３番８号
(72)発明者　豊田　清
東京都目黒区下目黒２丁目３番８号　松下電送システム株式会社内
(72)発明者　村田　松寿
東京都目黒区下目黒２丁目３番８号　松下電送システム株式会社内
(74)代理人　100105050
弁理士　鷲田　公一

最終頁に続く

(54)【発明の名称】暗号化メール配信システム

(57)【要約】
【課題】　高度な秘匿性と機密文書の緊急配信という相反する要求を達成できる暗号化メール配信システムを提供すること。
【解決手段】　メールサーバ９は、署名付メールを受信したならば、署名付メールの受信者が登録された受信側のセキュアＩＦＡＸアダプタ２３Ｂに対して着信通知メールを送信し、受信側のセキュアＩＦＡＸアダプタ２３Ｂは、着信通知メールを受信したならばその宛先アカウントからその所有者である受信者に対して暗号化メールの着信を通報し、ＩＣカード１０９を用いて受信者の個人認証を行うことを要求し、受信者の確認が取れた後署名付メールを受信、復号化する。これにより、署名付メールの機密文書をメールサーバ９から所望の受信者に迅速かつ確実に取り出させる。



1

【特許請求の範囲】

【請求項１】　電子メールに暗号化処理を施して暗号化メールとして送信する電子メール送信端末装置と、前記暗号化メールの宛先としての電子メール受信端末装置と、受信した電子メールを宛先毎に蓄積される電子メール受信端末装置からの要求に応じて当該電子メール受信端末装置宛ての電子メールを送信する電子メールサーバ装置と、で構成される暗号化メール配信システムであって、

前記電子メールサーバ装置は、前記暗号化メールを受信したならば前記暗号化メールの受信者が登録された電子メール受信端末装置に対して前記暗号化メールが着信した旨を通知する着信通知メールを直接送信する着信通知手段を具備し、

前記電子メール受信端末装置は、前記電子メールサーバ装置から着信通知メールを受信したならば前記受信者に対して前記暗号化メールの着信を通報する着信通知通報手段と、前記受信者の個人認証を行う個人認証手段と、前記個人認証手段によって前記受信者の確認が完了した後に前記暗号化メールの送信を前記電子メールサーバ装置に対して要求する電子メール受信手段と、前記電子メールの暗号化されたメッセージを復号化する復号化手段と、を具備することを特徴とする暗号化メール配信システム。

【請求項２】　電子メール受信端末装置は、ＩＣカードから情報を読み出すカードリーダ手段をさらに具備し、個人認証手段は、前記カードリーダ手段が前記ＩＣカードから読み出した情報を用いて個人認証を行うことを特徴とする請求項１記載の暗号化メール配信システム。

【請求項３】　電子メール受信端末装置は、ＩＣカードから情報を読み出すカードリーダ手段をさらに具備し、復号化手段は、前記ＩＣカードに格納された受信者の秘密鍵を用いて暗号化メールの復号化処理を行うことを特徴とする請求項１記載の暗号化メール配信システム。

【請求項４】　個人認証手段は、ＩＣカードに格納された受信者の証明書を読み出しその有効性を証明書サーバに問い合わせ、前記証明書が有効である場合に前記受信者が正常であることを確認することを特徴とする請求項２または請求項３記載の暗号化メール配信システム。

【請求項５】　電子メール送信端末装置は、送信者の個人認証を行う個人認証手段をさらに具備し、前記個人認証手段により送信者の個人認証の確認が終了した後、電子メールを暗号化し電子メールサーバ装置に送信することを特徴とする請求項１から請求項４のいずれかに記載の暗号化メール配信システム。

【請求項６】　電子メール送信端末装置は、ＩＣカードから情報を読み出すカードリーダ手段をさらに具備し、個人認証手段は、前記カードリーダ手段が前記ＩＣカードから読み出した情報を用いて個人認証を行うことを特徴とする請求項５記載の暗号化メール配信システム。

2

【請求項７】　電子メール送信端末装置は、証明書サーバから受信者情報を読み出す手段を具備し、暗号化手段は、前記受信者情報の公用鍵を用いて電子メールの暗号化処理を行うことを特徴とする請求項５記載の暗号化メール配信システム。

【請求項８】　個人認証手段は、ＩＣカードに格納された送信者の証明書を読み出しその有効性を証明書サーバに問い合わせ、前記証明書が有効である場合に前記送信者が正常であることを確認することを特徴とする請求項６または請求項７記載の暗号化メール配信システム。

【請求項９】　電子メール受信端末装置は、暗号化メールを受信後、送達確認通知を電子メール送信端末装置に送信することを特徴とする請求項１から請求項８のいずれかに記載の暗号化メール配信システム。

【請求項１０】　電子メール送信端末装置は、送達確認通知を受信したならばその内容を出力する出力手段を具備することを特徴とする請求項９記載の暗号化メール配信システム。

【請求項１１】　出力手段は、送達確認通知が所定の数だけ受信したならばそれらの内容をまとめて出力することを特徴とする請求項１０記載の暗号化メール配信システム。

【請求項１２】　電子メール送信端末装置は、送達確認通知を受信したならば、履歴管理サーバに暗号化メールの送信履歴を登録することを特徴とする請求項９から請求項１１のいずれかに記載の暗号化メール配信システム。

【請求項１３】　送信元の電子メール送信端末装置からの電子メールを配信するメールサーバ装置であって、前記電子メールを蓄積する蓄積手段と、前記蓄積手段に蓄積した電子メールが所定の電子メールである場合には当該所定の電子メールの宛先に対して着信通知を行う通知手段と、前記宛先から要求があったならば前記蓄積手段に蓄積した前記所定の電子メールを前記宛先に送信する送信手段と、を備えることを特徴とするメールサーバ装置。

【請求項１４】　所定の電子メールは、送信元で電子メールに署名処理を施した署名付きメールであることを特徴とする請求項１３記載のメールサーバ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化メール配信システムに関する。

【０００２】

【従来の技術】近年、一般的なファクシミリと同様の操作で画情報をインターネット経由で送信するファクシミリ装置が開発されている。この種のファクシミリは、通信経路の全部または一部にインターネットを使用することからインターネットファクシミリ端末装置（以下、「ＩＦＡＸ端末」という）と呼ばれている。

【０００３】このようなＩＦＡＸ端末は、ファクシミリデータを電子メールのフォーマットに変換して送信する。具体的には、ＩＦＡＸ端末は、読み取った原稿をＭＨデータに変換し、そのMHデータをＴＩＦＦファイルに変換する。さらに、そのＴＩＦＦファイルをテキストコード変換し、そのテキストコード変換されたデータをＭＩＭＥ形式に従ったデータに変換して送信を行っている。

【０００４】ＩＦＡＸ端末は、一人の者が占有するというよりも職場において同一の部署に属する複数の者によって共用されるのが一般的である。また、ＩＦＡＸ端末宛ての電子メールは、ＩＦＡＸ端末が自動的に受信し、印刷するため、送信側が指定した特定の個人以外の目に触れるおそれがあるので、通常のパーソナルコンピュータ等の一人の者が占有するメール受信端末に比べて秘匿性が低いと考えられている。

【０００５】秘匿性の向上を目的として、ＩＦＡＸ端末に、電子メールの傍受、改竄およびなりすましを防止する技術として電子署名や情報暗号化の技術を採用することが行われている。このタイプのＩＦＡＸ端末を“セキュア（Secure）ＩＦＡＸ”と呼んでいる。従来のセキュアＩＦＡＸはＩＣカードリーダを搭載し、送信側でＩＣカードから電子署名や情報暗号化に必要な情報（例えば、公開鍵、秘密鍵など）を読み出し、これを用いて電子メールに電子署名処理または情報暗号化処理を施した後送信する。受信側では、電子メールで指示された個人が自己のＩＣカードをスロットに挿入し、これから読み出した公開鍵、秘密鍵などを用いて電子メールを復号化し、印刷する。このようにして、ＩＣカードの所有者以外のものが電子メールを傍受することを防止している。

【０００６】

【発明が解決しようとする課題】しかしながら、従来のセキュアＩＦＡＸにおいては、ＩＣカードの所有者だけが電子メールの受信を行うことができるようにするために、ＩＣカードに記憶した所有者のメールアカウントおよびパスワードを用いてＰＯＰサーバにログオンし、所有者のセキュアＩＦＡＸから電子メールを受信することが考えられる。この場合、ＩＣカードがスロットに挿入されていることがメール受信の必須条件となる。これでは、定期的にＰＯＰサーバにアクセスし、最新のメールを受信するためには、ＩＣカードを常時スロットに挿入していなくてはならない。これでは却って秘匿性が低下してしまうので、秘匿性を保ちながら機密文書をできる限り早くよりリアルタイムに受信することは難しい。また、ＩＣカードなしでＰＯＰサーバに接続可能とするために、セキュアＩＦＡＸ本体にメールアカウントおよびパスワードを格納する場合も同様に高度の秘匿性を達成し得ない。このように従来のセキュアＩＦＡＸでは、高度な秘匿性と機密文書の緊急配信という相反する要求を達成することができない。

【０００７】本発明は、かかる点に鑑みてなされたものであり、高度な秘匿性と機密文書の緊急配信という相反する要求を達成することができる暗号化メール配信システムを提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明は、上記課題を解決するために、電子メール送信端末装置が、電子メールに暗号化処理を施して暗号化メールとして送信し、電子メールサーバ装置は、暗号化メールを受信したならば暗号化メールの受信者が登録された電子メール受信端末装置に対して暗号化メールが着信した旨を通知する着信通知メールを直接送信し、電子メール受信端末装置は、電子メールサーバ装置から着信通知メールを受信したならば受信者に対して暗号化メールの着信を通報し、受信者の個人認証により受信者の確認が完了した後に暗号化メールの送信を電子メールサーバ装置に対して要求し、暗号化メールを受信し復号化することとした。これにより、高度な秘匿性と機密文書の緊急配信という相反する要求を達成することができる。

【０００９】

【発明の実施の形態】本発明の第１の態様は、電子メールに暗号化処理を施して暗号化メールとして送信する電子メール送信端末装置と、前記暗号化メールの宛先としての電子メール受信端末装置と、受信した電子メールを宛先毎に蓄積しある電子メール受信端末装置からの要求に応じて当該電子メール受信端末装置宛ての電子メールを送信する電子メールサーバ装置と、で構成される暗号化メール配信システムであって、前記電子メールサーバ装置は、前記暗号化メールを受信したならば前記暗号化メールの受信者が登録された電子メール受信端末装置に対して前記暗号化メールが着信した旨を通知する着信通知メールを直接送信する着信通知手段を具備し、前記電子メール受信端末装置は、前記電子メールサーバ装置から着信通知メールを受信したならば前記受信者に対して前記暗号化メールの着信を通報する着信通知通報手段と、前記受信者の個人認証を行う個人認証手段と、前記個人認証手段によって前記受信者の確認が完了した後に前記暗号化メールの送信を前記電子メールサーバ装置に対して要求する電子メール受信手段と、前記電子メールの暗号化されたメッセージを復号化する復号化手段と、を具備する構成を採る。

【００１０】本発明の第２の態様は、第１の態様において、電子メール受信端末装置は、ＩＣカードから情報を読み出すカードリーダ手段をさらに具備し、個人認証手段は、前記カードリーダ手段が前記ＩＣカードから読み出した情報を用いて個人認証を行うこととした。

【００１１】本発明の第３の態様は、第１の態様において、電子メール受信端末装置は、ＩＣカードから情報を読み出すカードリーダ手段をさらに具備し、復号化手段は、前記ＩＣカードに格納された受信者の秘密鍵を用い

て暗号化メールの復号化処理を行うこととした。

【００１２】本発明の第４の態様は、第２、３の態様において、個人認証手段は、ＩＣカードに格納された受信者の証明書を読み出しその有効性を証明書サーバに問い合わせ、前記証明書が有効である場合に前記受信者が正常であることを確認することとした。

【００１３】これらの構成により、電子メールサーバ装置は暗号化メールを受信したならば暗号化メールの受信者が登録された電子メール受信端末装置に対して暗号化メールが着信した旨を通知し、かつ、この通知を受けた電子メール受信端末装置は受信者に対して暗号化メールの着信を通知し、受信者の個人認証を行うことを要求し、受信者の確認が取れた後、暗号化メールを受信、復号化するので、暗号化メールの機密文書を電子メールサーバ装置から所望の受信者に迅速かつ確実に取り出させることができる。

【００１４】本発明の第５の態様は、第１から第４の態様のいずれかにおいて、電子メール送信端末装置は、送信者の個人認証を行う個人認証手段をさらに具備し、前記個人認証手段により送信者の個人認証の確認が終了した後、電子メールを暗号化し電子メールサーバ装置に送信することとした。

【００１５】本発明の第６の態様は、第５の態様において、電子メール送信端末装置は、ＩＣカードから情報を読み出すカードリーダ手段をさらに具備し、個人認証手段は、前記カードリーダ手段が前記ＩＣカードから読み出した情報を用いて個人認証を行うこととした。

【００１６】本発明の第７の態様は、第５の態様において、電子メール送信端末装置は、証明書サーバから受信者情報を読み出す手段を具備し、暗号化手段は、前記受信者情報の公用鍵を用いて電子メールの暗号化処理を行うこととした。

【００１７】本発明の第８の態様は、第６または第７の態様において、個人認証手段は、ＩＣカードに格納された送信者の証明書を読み出しその有効性を証明書サーバに問い合わせ、前記証明書が有効である場合に前記送信者が正常であることを確認することとした。

【００１８】これらの構成により、電子メール送信端末装置は、個人認証を行い、送信者の確認を取った後、電子メールを暗号化して宛先に送信するので、不正な送信者による機密文書の配信を未然に防止することができる。

【００１９】本発明の第９の態様は、第１から第８の態様のいずれかにおいて、電子メール受信端末装置は、暗号化メールを受信後、送達確認通知を電子メール送信端末装置に送信することとした。

【００２０】本発明の第１０の態様は、第９態様において、電子メール送信端末装置は、送達確認通知を受信したならばその内容を出力する出力手段を具備することとした。

【００２１】本発明の第１１の態様は、第１０の態様において、出力手段は、送達確認通知が所定の数だけ受信したならばそれらの内容をまとめて出力することとした。

【００２２】本発明の第１２の態様は、第９から第１１の態様のいずれかにおいて、電子メール送信端末装置は、送達確認通知を受信したならば、履歴管理サーバに暗号化メールの送信履歴を登録することとした。

【００２３】これらの構成により、電子メール受信端末装置は、暗号化メールを正常に受信したならば、送達確認通知を電子メール送信端末装置に返し、電子メール送信端末装置はこれを出力したり、送信履歴を履歴管理サーバに登録するので、機密文書の配信があったことを送信者が確認したり、その後第三者などが送信履歴を容易に確認することができる。

【００２４】本発明の第１３の態様に係るメールサーバ装置は、送信元の電子メール送信端末装置からの電子メールを配信し、前記電子メールを蓄積する蓄積手段と、前記蓄積手段に蓄積した電子メールが所定の電子メールである場合には当該所定の電子メールの宛先に対して着信通知を行う通知手段と、前記宛先から要求があったならば前記蓄積手段に蓄積した前記所定の電子メールを前記宛先に送信する送信手段と、を備える構成を採る。本発明の第１４の態様は、第１３の態様において、所定の電子メールは、送信元で電子メールに署名処理を施した署名付きメールであることとした。

【００２５】以下、本発明の実施の形態について図面を参照して詳細に説明する。図１は、本発明の一実施の形態に係る電子メール配信システムを示す概念図である。

【００２６】この電子メール配信システム１は、一つの管区局３と、その管理下にある複数の本部Ａ～本部Ｃと、それぞれの本部の管理下にある複数の支部Ａ１、Ａ２、Ｂ１、Ｂ２、Ｃ１、Ｃ２とで構成されている。これらは、ＷＡＮ５で接続されている。

【００２７】管区局３には、履歴管理サーバ７、メールサーバ９、証明書サーバ１０が設けられたＬＡＮ１１が構築されている。また、各本部Ａ～Ｃには、メールサーバ９がそれぞれ設けられたＬＡＮ１３、１５、１７がそれぞれ構築されている。これらのＬＡＮ１１～１７は、ルーター１９を介してＷＡＮ５に接続している。

【００２８】本部Ａ～Ｃおよび支部Ａ１～Ｃ２には、それぞれＩＦＡＸ端末２１が設置され、それにはセキュアＩＦＡＸアダプタ２３が接続されている。支部Ａ１～Ｃ２に設置されたセキュアＩＦＡＸアダプタ２３は、ルーター１９を介してＷＡＮ２５に接続する。セキュアＩＦＡＸアダプタ２３は、表示モニタ２７、スピーカ２９および表示灯３１を備えている。

【００２９】図２は、上記実施の形態に係るセキュアＩＦＡＸアダプタのハードウエア構成を示すブロック図である。セキュアＩＦＡＸアダプタ２３において、中央処

理部（ＣＰＵ）１０１は、各種プログラムを実行してセキュアＩＦＡＸアダプタ２３の各部を制御する。ＲＯＭ１０３は、ＣＰＵ１０１が実行するプログラムを格納する。ＲＡＭ１０５は、プログラムのデータ領域として使用されると共に、所定のデータを格納するメモリとして使用される。

【００３０】ＩＣカードＲＥＡＤ／ＷＲＩＴＥ部（以下、「ＩＣカードＲ／Ｗ部」という）１０７は、図示しないＩＣカードスロットに装着されたＩＣカード１０９に所定のデータの書込み、あるいは、ＩＣカード１０９に書込まれたデータの読取りを行う。

【００３１】第１ＬＡＮインタフェース（以下、「第１ＬＡＮＩ／Ｆ」という）１１１は、ＬＡＮ１１～１７とのデータの送受信を制御するインタフェースである。ＬＡＮ１１～１７に代わってルーター１９に直接接続されても良い。第２ＬＡＮインタフェース（以下、「第２ＬＡＮＩ／Ｆ」という）１１３は、ＩＦＡＸ端末２１とのデータの送受信を制御するインタフェースである。

【００３２】外部入出力インタフェース（以下、「外部Ｉ／Ｏ」という）１１５は、表示モニタ２７、スピーカ２９および表示灯３１に接続するためのインタフェースである。

【００３３】バス１１７は、ＣＰＵ１０１、ＲＯＭ１０３、ＲＡＭ１０５、ＩＣカードＲ／Ｗ部１０７、第１ＬＡＮＩ／Ｆ１１１、第２ＬＡＮＩ／Ｆ１１３および外部Ｉ／Ｏ１１５間でデータが転送される経路である。

【００３４】図３は、上記実施の形態に係るセキュアＩＦＡＸアダプタの主要な機能を示すブロック図である。信号種別判別部３０３は、ＩＦＡＸ端末２１から電子メールデータを送信する処理において、第２ＬＡＮＩ／Ｆ１１３から出力される所定のコマンド信号（応答信号）、または、ＬＡＮ１１～１７から電子メールデータを受信する処理において、第１ＬＡＮＩ／Ｆ１１１から出力される所定のコマンド信号（応答信号）の種別を判別する。所定のコマンド信号を判別した場合、信号種別判別部３０３は、第２ＬＡＮＩ／Ｆ１１３および第１ＬＡＮＩ／Ｆ１１１から続いて電子メールデータが出力されることを認識し、その旨をメールデータ通信部３０１に通知する。

【００３５】なお、所定のコマンド信号（応答信号）は、ＩＦＡＸ端末２１から電子メールデータを送信する処理においては、メールサーバ９から出力される“３５４”という応答信号である。一方、ＬＡＮ１１～１７から電子メールデータを受信する処理においては、メールサーバ９に対して出力した“ＲＥＴＲ”の後にメールサーバ９から出力されるＯＫレスポンスである。

【００３６】メールデータ通信部３０１は、信号種別判別部３０３より、電子メールデータが出力される旨の通知を受けた場合に、第１ＬＡＮＩ／Ｆ１１１および第２ＬＡＮＩ／Ｆ１１３から電子メールデータを受信する。また、メールデータ通信部３０１は、後述するカード情報判定部３０５から受け取った電子メールアドレス情報に基づいて電子メールデータの送受信処理を行う。

【００３７】カード情報判定部３０５は、ＩＣカードスロット３０７に装着されたＩＣカード１０９からＩＣカードＲ／Ｗ部１０７が読み取った情報の内容を判定する。そして、ＩＣカード１０９に署名処理または署名暗号化処理に必要な情報が格納されている場合に署名暗号化処理部３０９にその情報を与える。

【００３８】また、カード情報判定部３０５は、ＩＣカードＲ／Ｗ部１０７が読み取った情報に基づいてＩＣカード１０９の装着の有無についても判定する。さらに、カード情報判定部３０５は、ＩＣカード１０９に格納された電子メールアドレス情報を判定し、その電子メールアドレス情報をメールデータ通信部３０１に通知する。

【００３９】署名暗号化処理部３０９は、カード情報判定部３０５から受け取った署名暗号化処理等に必要な情報に基づいて、メールデータ通信部３０１が受信した電子メールデータに対して署名暗号化処理等の処理を行う。また、署名暗号化処理部３０９は、カード情報判定部３０５から受け取った署名暗号化処理等に必要な情報に基づいて、メールデータ通信部３０１が受信した電子メールデータに施された署名暗号化処理等の解読処理を行う。

【００４０】ここで、ＩＣカード１０９に格納された情報について説明する。ＩＣカード１０９は、ＩＦＡＸ端末２１から電子メールを送信する各ユーザが所有するものであり、各所有者に付与された電子メールアドレス情報（宛先アカウント）が格納されている。すなわち、セキュアＩＦＡＸアダプタ２３にＩＣカード１０９が装着されているときのみ、各所有者は、自分の電子メールアドレスから電子メールを送信することができ、自分の電子メールアドレスに対する電子メールを受信することができる。

【００４１】また、ＩＣカード１０９は、署名処理又は署名暗号化処理に必要となる情報を格納する。すなわち、ＩＣカード１０９は、自分の秘密鍵情報および公開鍵情報を格納する。なお、送信先の公開鍵情報は、証明書サーバ１０から検索した後セキュアＩＦＡＸアダプタ２３のＲＡＭ１０５内に蓄積される。

【００４２】一方、ＩＦＡＸ端末２１は、例えば、特開平８－２４２３２６号公報に開示されているような、スキャナで読み取った画像を電子メールに変換し、ＬＡＮを介して送信すると共に、送信側で画像を変換した電子メールを受信し、元の画像に逆変換して印刷する装置をいう。ＩＦＡＸ端末２１の具体例を図４を参照して簡単に説明する。図４は、上記実施の形態に係るセキュアＩＦＡＸアダプタに接続されるＩＦＡＸ端末の構成を示すブロック図である。

【００４３】ＩＦＡＸ端末２１は、ＣＰＵ４０１、ＲＯ

Ｍ４０３、ＲＡＭ４０５に加えて、原稿をスキャンして画像を得るスキャナ部４０７、画像を例えばMHのような圧縮形式で圧縮画像データに圧縮し、逆に圧縮画像データを元の画像に伸長する圧縮・伸長部４０９と、セキュアＩＦＡＸアダプタ２３などに接続するＬＡＮＩ／Ｆ４１３、画像を印刷するプリンタ部４１５、宛先を入力するためのパネル部４１１、圧縮画像データを電子メールに変換するフォーマット変換部４１９および電子メールを圧縮画像データに逆変換するフォーマット逆変換部４２１を具備する。

【００４４】ＩＦＡＸ端末２１では、送信者がスキャナ部４０７の原稿載置台に原稿をセットし、パネル部４１１から宛先メールアドレスを入力してスタートボタンを押すと、原稿を読み取って画像データを得、この画像データを圧縮・伸長部４０９で圧縮して圧縮画像データとする。この圧縮画像データをフォーマット変換部４１９によりＭＩＭＥに従って電子メールの添付ファイルとしてコーディングした電子メールに変換する。この電子メールをＬＡＮＩ／Ｆ４１３を介してセキュアＩＦＡＸアダプタ２３へ送信する。

【００４５】一方、ＩＦＡＸ端末２１は、ＬＡＮＩ／Ｆ４１３を介して電子メールを受信したならば、電子メールに添付された圧縮画像データをデコードし、圧縮・伸長部４０９で伸長し、元の画像データに復元し、プリンタ部４１５で印刷する。

【００４６】本実施の形態では、上述のように送信側のＩＦＡＸ端末２１Ａおよびセキュアファクシミリアダプタ２３Ａによって電子メール送信端末装置が、受信側のＩＦＡＸ端末２１Ｂおよびセキュアファクシミリアダプタ２３Ｂによって電子メール受信端末装置が夫々構成されている。

【００４７】図５は、上記実施の形態に係るメールサーバのハードウエア構成を示すブロック図である。メールサーバ９において、ネットワーク接続部５０１は、ＬＡＮ１１、１３と接続するものである。メールボックス５０２は、ハードディスク等の二次記憶装置５０３内に設けられ、受信した電子メールデータを宛先ごとに記憶する。

【００４８】ＣＰＵ５０４は、コンピュータ等を動作させるものであり、ＲＡＭ５０５、ＲＯＭ５０６を用いて、受信した電子メールに対して図９に示す処理を行う。

【００４９】宛先認識部５０７は、受信した電子メールデータの送信宛先を認識するものである。ここで送信宛先を認識できない場合、エラーメール作成部５０８に対してエラーメールの作成を指示する。

【００５０】メールデータ判断部５０９は、署名付きメールか否かにより電子メールデータの種別を判断し、署名付きメールであれば、着信メール作成部５１０に対して着信メールを作成させる。

【００５１】ＰＯＰ受信要求判断部５１１は、端末からのＰＯＰ受信要求があったか、否かを判断し、その要求があれば、電子メールボックス５０２に対して、その要求者のアカウントに基づいて対応するメールデータを送信する。アカウント管理部５１２は、メールサーバ９が自ら管理する電子メール受信端末装置のアカウントを管理する。

【００５２】以下、上記実施の形態に係る電子メール配信システムにおいて、本部Ａから本部Ａ１にそれぞれ設置したＩＦＡＸ端末２１およびセキュアＩＦＡＸアダプタ２３間で電子メールを送受信した場合を例に挙げて説明する。

【００５３】図６は、上記実施の形態に係る電子メール配信システムでのメール配信シーケンスを示す図である。図７は、上記実施の形態に係る電子メール配信システムでの送信側のセキュアＩＦＡＸアダプタの動作を示すフロー図である。図８は、上記実施の形態に係る電子メール配信システムでの送信側のＩＦＡＸ端末でのメール送信動作を示すフロー図である。図９は、上記実施の形態に係る電子メール配信システムでのメールサーバのメール配信動作を示すフロー図である。図１０は、上記実施の形態に係る電子メール配信システムでの受信側のセキュアＩＦＡＸアダプタの動作を示すフロー図である。

【００５４】図６に示すように、本実施の形態による電子メール配信は、送信者がＩＣカード１０９を送信側のセキュアＩＦＡＸアダプタ２３ＡのＩＣカードスロット３０７に挿入することから始まる。図７に示すように、ＩＣカード１０９が挿入されると（ステップ（以下、ＳＴという）６０１）、証明書サーバ１０に、ＩＣカード１０９に記憶された証明書が有効か否かの確認を問い合わせる（ＳＴ６０２）。問い合わせ結果が有効であるか否か判定し（ＳＴ６０３）、有効であれば送信側のＩＦＡＸ端末２３Ａからのメッセージの送信を待つ（ＳＴ６０４）。

【００５５】なお、セキュアＩＦＡＸアダプタ２３Ａで、証明書の確認処理が完了するする前に、ＩＦＡＸ端末２１Ａからメッセージが送信される場合が考えられる。このときには、送信されたメッセージを、セキュアＩＦＡＸアダプタ２３Ａ内に一旦取り込んでおき、証明が確認された後に、自動的にメッセージ送信を行うようにする。この構成により、ＩＦＡＸ端末２１Ａとセキュアファクシミリアダプタ２３Ａとの間で、証明書確認のための通信を行う必要がなく、既存のＩＦＡＸ端末を用いることできる。一方で、セキュアＩＦＡＸアダプタ２３Ａから確認処理が完了した旨の通知をＩＦＡＸ端末２１Ａが受けると、ＩＦＡＸ端末２１Ａ側内で待機されたメッセージが送信されるようにしても良い。この構成では、セキュアＩＦＡＸアダプタ２３Ａにデータを取り込むことを必要としないため、余計なメモリを要せず、また確

認証明が完了した後に、送信が実行がなされるため、確実な処理を行うことができるものである。

【００５６】送信側のＩＦＡＸ端末２３Ａでは、図８に示すように、パネル部４１１から宛先が指定された後（ＳＴ７０１）、パネル部４１１に設けられたスタートボタン（図示せず）が押し下げられると（ＳＴ７０２）、スキャナ部４０７で原稿を読み取り（ＳＴ７０３）、得られた画像データを圧縮・伸長部４０９で圧縮し（ＳＴ７０４）、フォーマット変換部４１９でＴＩＦＦ－Ｆフォーマットに変換し（ＳＴ７０５）、メッセージを作成する。このメッセージには宛先アドレスが含まれている。その後、メッセージをＬＡＮＩ／Ｆ４１３からセキュアＩＦＡＸアダプタ２３Ａに送信する（ＳＴ７０６）。

【００５７】図７に戻って、ＳＴ６０４において、セキュアＩＦＡＸアダプタ２３Ａは、ＩＦＡＸ端末２１Ａからメッセージを受信したならば、メッセージから宛先アドレスを取得する（ＳＴ６０５）。この宛先アドレスを使って証明書サーバ１０に宛先証明書を要求する（ＳＴ６０６）。証明書サーバ１０はリポジトリ検索を行い、宛先証明書を発行する。リポジトリ検索とは、宛先アドレスから証明書サーバ１０に保存されている宛先証明書を検査することをいう。セキュアＩＦＡＸアダプタ２３Ａは、証明書を取得したか否か判定し（ＳＴ６０７）、所得したならば、ＩＦＡＸ端末２１Ａから受信したメッセージに対して電子署名処理（ＳＴ６０８）、および暗号化処理（ＳＴ６０９）を施して、署名暗号化処理された電子メール（以下、「署名付メール」という）を作成する。

【００５８】より具体的には、図３に示す署名暗号化処理部３０９が、証明書サーバ１０からの宛先証明書（公開鍵情報）を入手する。一方、カード情報判定部３０５は、ＩＣカード１０９に格納されている自己の秘密鍵情報を署名暗号化処理部３０９に渡す。署名暗号化処理部３０９は、この自己の証明書（秘密鍵情報）および宛先の証明書（公開鍵情報）を用いて署名暗号化処理を行う。

【００５９】さらに詳細に説明すると、まずメッセージからハッシュ関数等の不可逆性の関数で演算処理を行い、メッセージダイジェストを取り出し、そのメッセージダイジェストに自己の秘密鍵情報を用いて暗号化処理を施す。さらに、ＤＥＫ（DataEncryption Key）と呼ばれる擬似乱数を用いた暗号鍵を生成する。そして、そのＤＥＫに対して送信先の公開鍵情報を用いて暗号化処理を施す。一方、先に暗号化処理を施したメッセージダイジェスト（署名結果）および電子メールのメッセージに対して、そのＤＥＫで所定の暗号化方式（例えば、ＤＥＳ：Data Encryption Standard）にしたがって暗号化処理を施す。

【００６０】ＳＴ６０７において宛先証明書を取得できない場合には、ＩＦＡＸ端末２１Ａにエラーを通知し（ＳＴ６１１）、処理を終了している。しかし、カード情報判定部３０５が、ＩＣカード１０９に格納されている自己の秘密鍵情報を署名暗号化処理部３０９に渡し、署名暗号化処理部３０９は、この自己の秘密鍵情報を用いて署名処理を行うようにしても良い。

【００６１】このようにして作成された署名付メールをメールサーバ９に宛てて送信し（ＳＴ６１０）、送信が正常に完了したか否か判定する（ＳＴ６１２）。正常に完了しない場合にはＩＦＡＸ端末２１Ａにエラーを通知する（ＳＴ６１１）。

【００６２】一方、ＳＴ６０３において、証明書が無効であった場合、表示モニタ２７にＩＣカードが無効である旨のメッセージを表示し（ＳＴ６１３）、ＩＦＡＸ端末２１Ａからメッセージ送信があったならば（ＳＴ６１４）、ＩＦＡＸ端末２１Ａにエラーを通知する（ＳＴ６１５）。

【００６３】図８に戻って、送信側のＩＦＡＸ端末２１Ａは、ＳＴ７０６でメッセージを送信した後、セキュアＩＦＡＸアダプタ２３Ａでエラーがあったか否かを監視し（ＳＴ７０７）、エラーがなければ送信が正常終了した旨のメッセージをパネル部４１１のＬＣＤ（図示せず）に表示し（ＳＴ７０８）、エラーがあればその旨を表示する（ＳＴ７０９）。

【００６４】送信側のセキュアＩＦＡＸアダプタ２３Ａから署名付メールを含む、種々の電子メールをメールサーバ９が受信する。図９に示すように、メールサーバ９は、接続要求があったならば（ＳＴ８０１）、電子メール受信を行う（ＳＴ８０２）。これは例えばＳＭＴＰプロトコルにより行われる。電子メール受信でエラーが発生したか否か判定し（ＳＴ８０３）、エラーがあれば送信元にエラー通知メールを送信し（ＳＴ８０４）、処理を終了する。一方、エラーがなければ、電子メールの宛先アカウントを自らが管理しているか否か判定する（ＳＴ８０５）。宛先アカウントを管理していないならば、受信した電子メールを他のサーバに転送し（ＳＴ８０６）、処理を終了する。

【００６５】自らが管理している宛先アカウントであれば、電子メールの種別を判定する（ＳＴ８０７）。判定は、具体的には、次のように行う。メールヘッダを解析して送達確認のヘッダ、すなわち“context-type:multipart/report:”があれば送達確認メールとみなす。

【００６６】判定が終了したならば、判定の結果に基づいて電子メールが送達確認メールか否か判定する（ＳＴ８０８）。送達確認メールについては後述する。

【００６７】送達確認メールでなかったならば、電子メールを宛先アカウントに対応するメールアダプタに格納する（ＳＴ８０９）。次いで、電子メールが署名付メールか否か判定し（ＳＴ８１０）、署名付メールであれば、その着信を受信側のセキュアＩＦＡＸアダプタ２３

Ｂに通知する着信通知メールを作成する（ＳＴ８１１）。この着信通知メールは、署名付メールの宛先アカウント（宛先メールアドレス）と同一の宛先に宛てて送信するため、宛先フィールド［Ｔｏ：］にはこの宛先アカウント（例えば、shibutyou@shibu.co.jp）が指定されている。メールサーバ９は、ＤＮＳにより受信側のＩＦＡＸアダプタ２３ＢのＩＰアドレスを認識し、これに宛ててＳＭＴＰプロトコルで着信通知メールを送信する（ＳＴ８１１）。

【００６８】なお、署名付メールであるか否かの判断は、メールヘッダに記述されている“Content-type”の欄に“ｓｉｇｎ”の文字列があることで判断する。

【００６９】受信側のセキュアＩＦＡＸアダプタ２３Ｂは、メールサーバ９からのメール受信の要求を常時待っている（ＳＴ９０１）。要求があったならば着信通知メールをＳＭＴＰプロトコルで受信する（ＳＴ９０２）。その後、着信通知メールを解析し、その宛先アドレスを所有する個人（以下、単に「受信者」という）宛てに着信付メールが着信していることを通報する（ＳＴ９０３）。この通報方法は特に限定されないが、具体的には、表示モニタ２７に着信通知のメッセージや受信者の名前を表示したり、スピーカ２９から音声により受信者の名前やメッセージを再生したり、表示灯３１を点灯させるなどにより行うことができる。この通報を受けて受信者はＩＣカード１０９をセキュアＩＦＡＸアダプタ２３Ｂのカードスロット３０７に挿入する。

【００７０】受信側のセキュアＩＦＡＸアダプタ２３Ｂは、ＩＣカード１０９の挿入を確認したならば（ＳＴ９０４）、ＩＣカード１０９の所有者情報と宛先とが一致するか否か判定する（ＳＴ９０５）。宛先が一致しなかったならば、エラー表示を行い（ＳＴ９０６）、一致するまでＳＴ９０３～ＳＴ９０５を繰り返す。宛先が一致したならば、ＩＣカード１０９から証明書を読み出し（ＳＴ９０７）、証明書サーバ１０に対して証明書が有効か否かの確認を問い合わせる（ＳＴ９０８）。その結果に基づいて証明書が有効か否か判断し（ＳＴ９０９）、有効であったならば、受信指示要求のメッセージを表示モニタ２７に表示する（ＳＴ９１０）。無効であった場合には、エラー表示を行い（ＳＴ９１１）、処理を終了する。

【００７１】受信者が受信側のＩＦＡＸ端末２１Ｂの受信指示ボタンをオンすると、セキュアＩＦＡＸアダプタ２３Ｂに対して受信指示信号が送信される。この受信指示がＩＦＡＸ端末２１Ｂからあったならば（ＳＴ９１２）、セキュアＩＦＡＸアダプタ２３Ｂは、メールサーバ９との間でＰＯＰ受信を行い、署名付メールを受信する（ＳＴ９１３）。このＰＯＰ受信には、ＩＣカード１０９内に格納された受信者のログインＩＤおよびパスワードが用いられる。

【００７２】セキュアＩＦＡＸアダプタ２３Ｂは、受信した署名付メールのデータを復号化する（ＳＴ９１４）。この復号化は、図３に示す署名暗号化処理部３０９が行う。具体的には、暗号化されているＤＥＫを自分の秘密鍵情報で復号化し、復号化したＤＥＫで暗号化されたデータを復号化する。そして、復号化したデータから、電子メールデータをメッセージダイジェストとメッセージデータに分離する。

【００７３】次いで、この復号化でエラーが発生したか否か判定し（ＳＴ９１５）、エラーがあったならば、エラー表示を行い（ＳＴ９１６）、処理を終了する。エラーがなく正常に復号化が行われたならば、証明書サーバ１０から送信者の証明書（公開鍵情報）を取得する（ＳＴ９１７）。そして、取得した公開鍵情報を用いて署名検証を行う（ＳＴ９１８）。署名検証処理も、署名暗号化処理部３０９が行うが、具体的には、復号化処理で得たメッセージダイジェストを送信者の公開鍵情報で復号化し、その結果を保持しておく。また、復号化処理で分離したメッセージデータから、上述したようなハッシュ関数を用いてメッセージダイジェストを抽出する。そして、そこで得たメッセージダイジェストと先ほど保持したメッセージダイジェストとを比較する。これにより、電子メールのメッセージデータが改ざんされていないか、また、正当な送信者から送信されたかを確認することができる。

【００７４】このような署名検証でエラー（すなわち、正当な送信者から改ざんなくメッセージが送信されていない）が起こったか否か判定し（ＳＴ９１９）、エラーがあったならばその旨を表示モニタ２７に表示して（ＳＴ９２０）、処理を終了する。エラーがなかったならば、復号化したデータをＩＦＡＸ端末２１Ｂに送信して印刷、表示などを行わせる（ＳＴ９２１）。次いで、送達確認メールを作成し、メールサーバ９にＳＭＴＰ送信する（ＳＴ９２２）。

【００７５】メールサーバ９は、送達確認メールを受信した場合、図９のＳＴ８０８において送達確認メールであることを認識し、送信元にＳＭＴＰプロトコルで転送する（ＳＴ８１３）。送達確認メールは、図６のシーケンス図に示すように、ＳＭＴＰプロトコルを用いて受信側のセキュアＩＦＡＸアダプタ２３Ｂ、メールサーバ９、送信側のセキュアＩＦＡＸアダプタ２３Ａを順次経由して、送信側のＩＦＡＸ端末２１Ａが受信し、送達レポートとして表示、印刷などで出力する。また、送信側のセキュアＩＦＡＸアダプタ２３Ａは、送達確認メールを受信したならばその旨を履歴管理サーバ７に登録する。

【００７６】以上説明したように、本実施の形態によれば、メールサーバ９は、署名付メール（すなわち、署名処理および暗号化が施された電子メール）を受信したならば、署名付メールの受信者が登録された受信側のセキュアＩＦＡＸアダプタ２３Ｂに対して着信通知メールを

送信し、受信側のセキュアＩＦＡＸアダプタ２３Ｂは、着信通知メールを受信したならばその宛先アカウントからその所有者である受信者に対して暗号化メールの着信を通報し、ＩＣカード１０９を用いて受信者の個人認証を行うことを要求し、受信者の確認が取れた後署名付メールを受信、復号化するので、署名付メールの機密文書をメールサーバ９から所望の受信者に迅速かつ確実に取り出させることができる。この結果、高度な秘匿性と機密文書の緊急配信という相反する要求を達成することができる。

【００７７】また、送信側のセキュアＩＦＡＸアダプタ２３Ａでは、ＩＣカード１０９を用いて証明書サーバ１０に証明書の有効性を確認することで個人認証を行い、送信者の確認を取った後、電子メールを署名処理および暗号化を施して宛先に送信するので、不正な送信者による機密文書の配信を未然に防止することができる。

【００７８】また、受信側のセキュアＩＦＡＸアダプタ２３Ｂは、署名付メールを正常に受信したならば、送達確認通知を送信側に返し、送信側のＩＦＡＸ端末２１Ａはこれを印刷したり、送信履歴を履歴管理サーバ７に登録するので、機密文書の配信があったことを送信者が確認したり、その後第三者などが送信履歴を容易に確認することができる。

【００７９】上述の本実施の形態では、ＩＦＡＸの基本的構成（画情報を電子メールで送受信する構成等）とセキュアＩＦＡＸの拡張部分構成（署名処理・暗号化処理等）とが別々の装置により実現されているが、これに限定されるものではなく、ＩＦＡＸ端末２１がセキュアＩＦＡＸアダプタ２３の機能を内蔵していても良い。

【００８０】また、本実施の形態では、個人認証にＩＣカード１０９に記憶された証明書を証明書サーバ１０で確認することで行っているが、これに代わって、音声認証、指紋認証等の他の一般的に知られている個人認証技術を用いても良いし、これと併有しても良い。しかしながら、本実施の形態で採用するＩＣカードを用いた個人認証は、公用鍵を用いた暗号化および秘密鍵による復号化を可能とする点で優れている。

【００８１】また、本実施の形態では、電子メールに署名処理および暗号化処理を施しているが、署名処理を行わず単に暗号化のみということもできる。よって、本発明は広く暗号化を施した電子メール、すなわち暗号化メールによる機密文書の配信に関するものである。

【００８２】本発明は、当業者に明らかなように、上記実施の形態に記載した技術にしたがってプログラムされた一般的な市販のデジタルコンピュータおよびマイクロプロセッサを使って実施することができる。また、当業者に明らかなように、本発明は、上記実施の形態に記載した技術に基づいて当業者により作成されるコンピュータプログラムを包含する。

【００８３】また、本発明を実施するコンピュータをプログラムするために使用できる命令を含む記憶媒体であるコンピュータプログラム製品が本発明の範囲に含まれる。この記憶媒体は、フロッピー（登録商標）ディスク、光ディスク、ＣＤ－ＲＯＭおよび磁気ディスク等のディスク、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気光カード、メモリカードまたはＤＶＤ等であるが、特にこれらに限定されるものではない。

【００８４】

【発明の効果】以上説明したように本発明によれば、電子メールサーバ装置は暗号化メールを受信したならば、暗号化メールの受信者が登録された受信側の電子メール受信端末装置に対してその着信を通知する着信通知メールを送信し、電子メール受信端末装置は、着信通知メールを受信したならばその宛先アカウントからその所有者である受信者に対して暗号化メールの着信を通報し、受信者の個人認証を行うことを要求し、受信者の確認が取れた後暗号化メールを受信、復号化するので、暗号化メールの機密文書を電子メールサーバ装置から所望の受信者に迅速かつ確実に取り出させることができる等効果を奏するものである。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る電子メール配信システムを示す概念図

【図２】上記実施の形態に係るセキュアＩＦＡＸアダプタのハードウエア構成を示すブロック図

【図３】上記実施の形態に係るセキュアＩＦＡＸアダプタの主要な機能を示すブロック図

【図４】上記実施の形態に係るセキュアＩＦＡＸアダプタに接続されるＩＦＡＸ端末の構成を示すブロック図である。

【図５】上記実施の形態に係るメールサーバのハードウエア構成を示すブロック図

【図６】上記実施の形態に係る電子メール配信システムでのメール配信シーケンスを示す図

【図７】上記実施の形態に係る電子メール配信システムでの送信側のセキュアＩＦＡＸアダプタの動作を示すフロー図

【図８】上記実施の形態に係る電子メール配信システムでの送信側のＩＦＡＸ端末でのメール送信動作を示すフロー図

【図９】上記実施の形態に係る電子メール配信システムでのメールサーバのメール配信動作を示すフロー図

【図１０】上記実施の形態に係る電子メール配信システムでの受信側のセキュアＩＦＡＸアダプタの動作を示すフロー図

【符号の説明】

１　電子メール配信システム
７　履歴管理サーバ
９　メールサーバ
１０　証明書サーバ

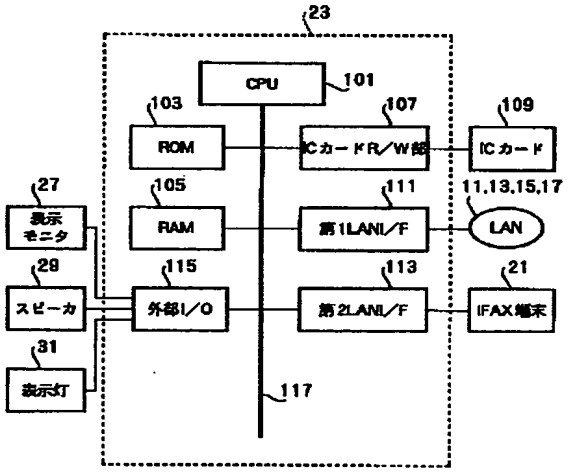
17

２１、２１Ａ、２１Ｂ　ＩＦＡＸ端末
２３、２３Ａ、２３Ｃ　セキュアＩＦＡＸアダプタ
２７　表示モニタ
２９　スピーカ
３１　表示灯
１０７　ＩＣカードＲ／Ｗ部
１０９　ＩＣカード
３０１　メールデータ通信部
３０３　信号種別判別部
３０５　カード情報判定部
３０７　カードスロット
３０９　署名暗号化処理部
４０７　スキャナ部
４０９　圧縮・伸長部
４１１　パネル部

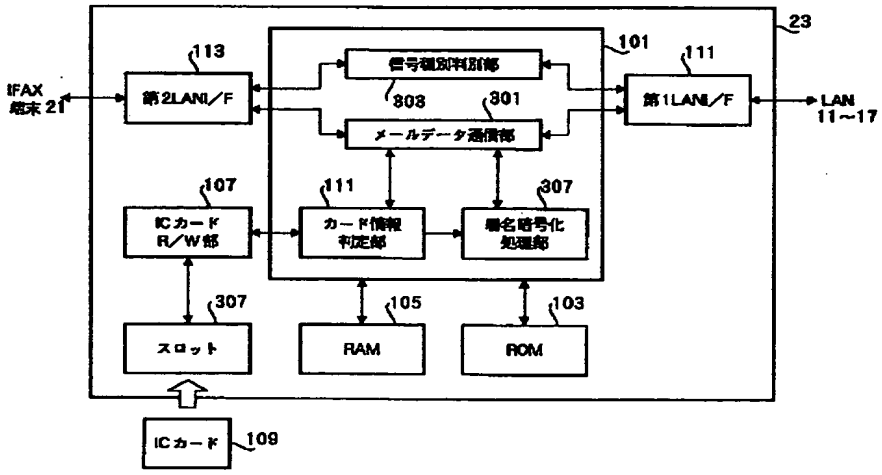
18

４１５　プリンタ部
４１９　フォーマット変換部
４２１　フォーマット逆変換部
５０１　ネットワーク接続部
５０２　メールボックス
５０３　二次記憶装置
５０４　ＣＰＵ
５０５　ＲＡＭ
５０６　ＲＯＭ
５０７　宛先認識部
５０８　エラーメール作成部
５０９　メールデータ判断部
５１０　着信メール作成部
５１１　ＰＯＰ受信要求判断部
５１２　アカウント管理部

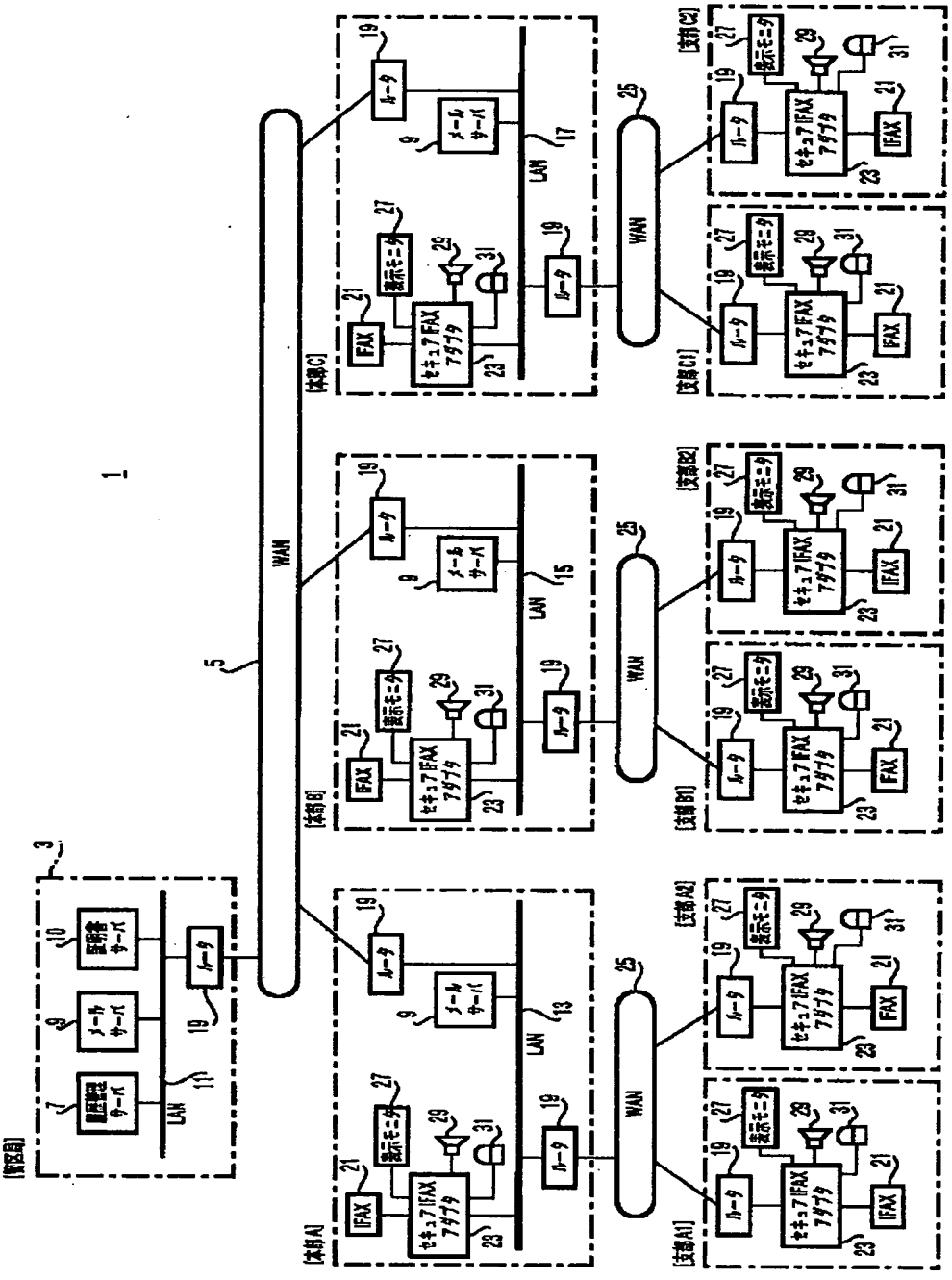
【図２】



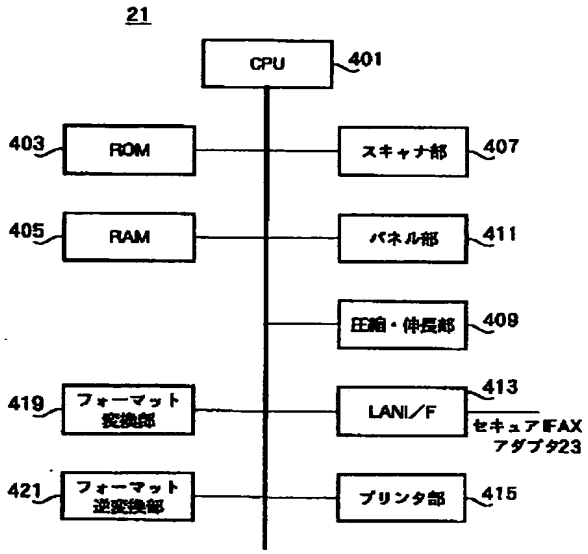
【図３】



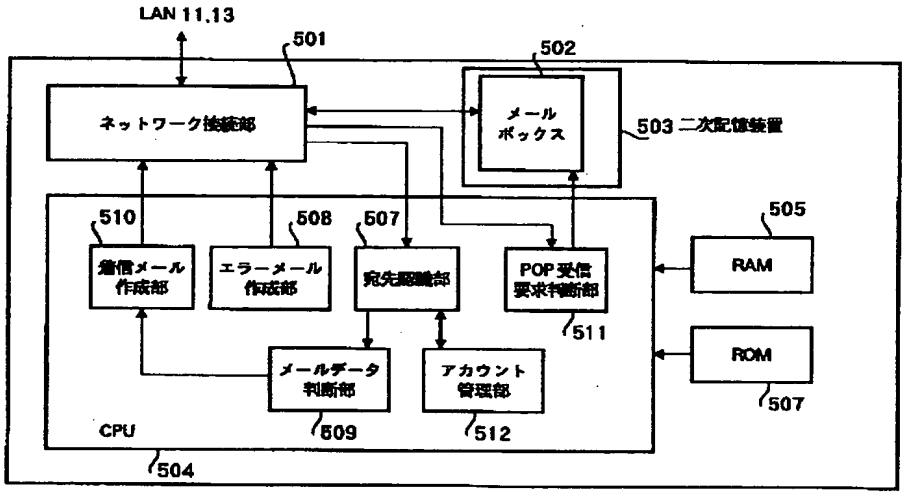
【図１】


1
3
5
WAN
LAN
ルータ
メールサーバ
FAX
IFAX
表示モニタ
セキュアIFAXアダプタ
[管理局]
[本部A]
[本部B]
[本部C]
[支部A1]
[支部A2]
[支部B1]
[支部B2]
[支部C1]
[支部C2]

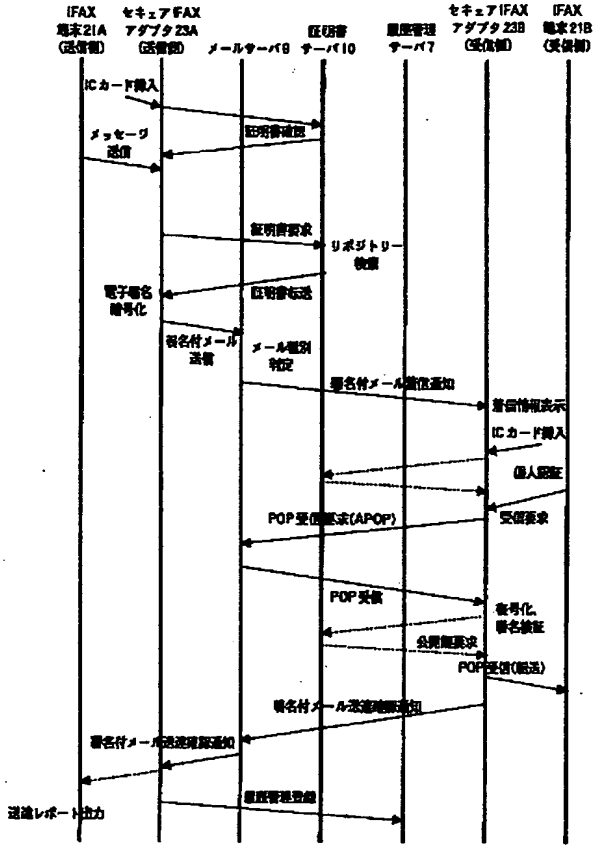
【図４】


21
CPU
401
403
ROM
407
スキャナ部
405
RAM
411
パネル部
409
圧縮・伸長部
419
フォーマット変換部
413
LANI／F
セキュアFAX アダプタ23
421
フォーマット逆変換部
415
プリンタ部

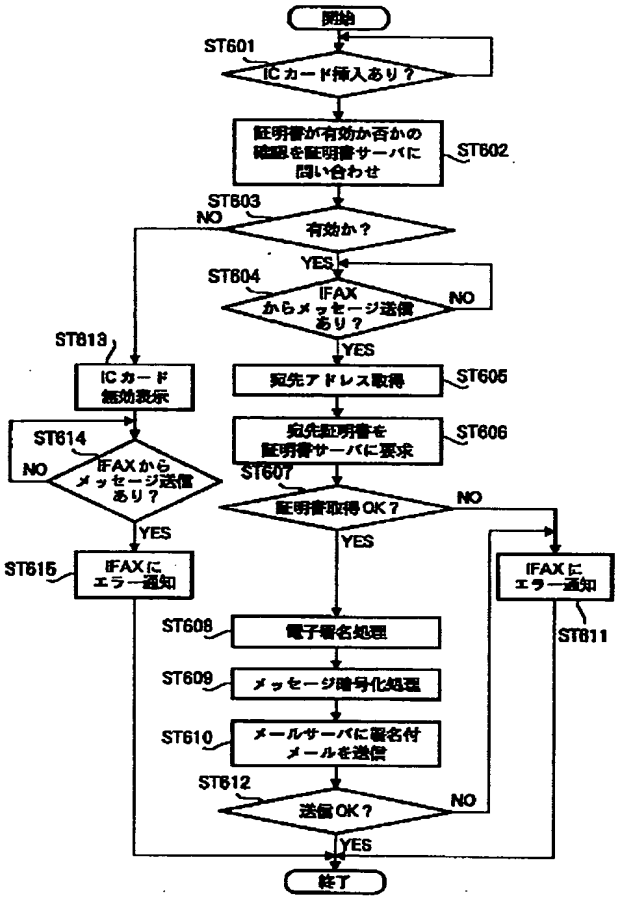
【図５】


LAN 11,13
501
502
ネットワーク接続部
メールボックス
503 二次記憶装置
510
508
507
505
着信メール作成部
エラーメール作成部
宛先認識部
POP受信要求判断部
RAM
511
メールデータ判断部
アカウント管理部
ROM
507
CPU
509
512
504

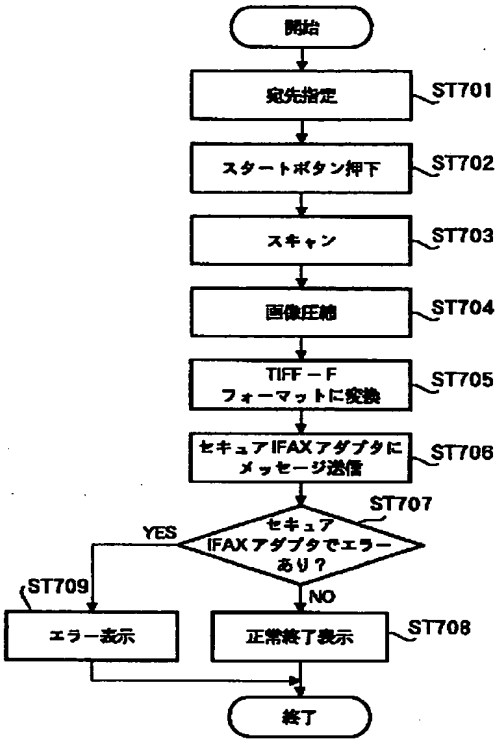
【図６】


IFAX
端末21A
(送信側)
セキュアIFAX
アダプタ23A
(送信側)
メールサーバ8
証明書
サーバ10
履歴管理
サーバ7
セキュアIFAX
アダプタ23B
(受信側)
IFAX
端末21B
(受信側)
ICカード挿入
メッセージ
送信
証明書要求
リポジトリー
検索
証明書転送
電子署名
暗号化
署名付メール
送信
メール種別
判定
署名付メール着信通知
着信情報表示
ICカード挿入
個人認証
受信要求
POP受信要求(APOP)
POP受信
復号化、
署名検証
公開鍵要求
POP受信(転送)
署名付メール送達確認通知
署名付メール送達確認通知
履歴管理登録
送達レポート出力

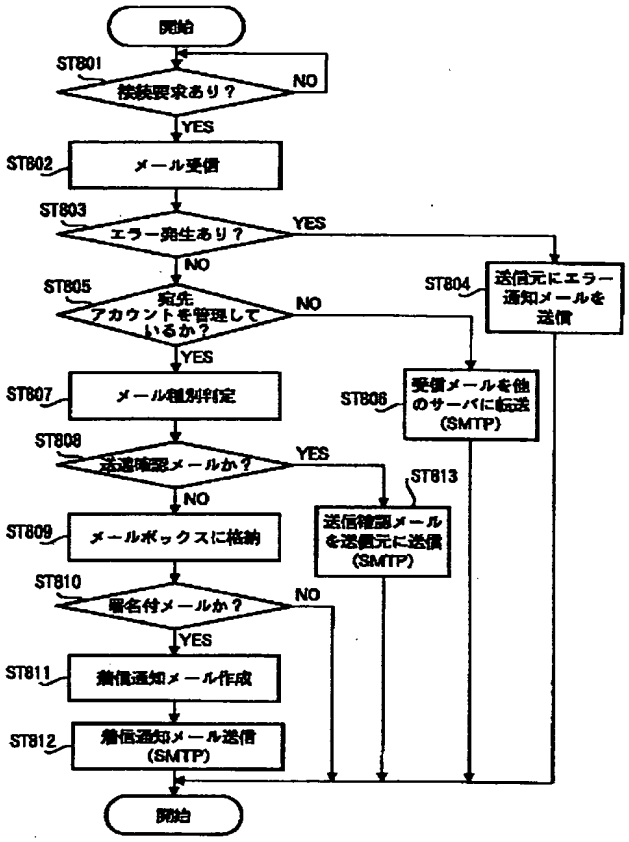
【図７】


開始
ST601
ICカード挿入あり？
証明書が有効か否かの
確認を証明書サーバに
問い合わせ
ST602
ST603
NO
有効か？
YES
ST604
IFAX
からメッセージ送信
あり？
NO
YES
ST613
ICカード
無効表示
宛先アドレス取得
ST605
宛先証明書を
証明書サーバに要求
ST606
ST614
NO
IFAXから
メッセージ送信
あり？
ST607
証明書取得OK？
NO
YES
YES
ST615
IFAXに
エラー通知
IFAXに
エラー通知
ST611
ST608
電子署名処理
ST609
メッセージ暗号化処理
ST610
メールサーバに署名付
メールを送信
ST612
送信OK？
NO
YES
終了

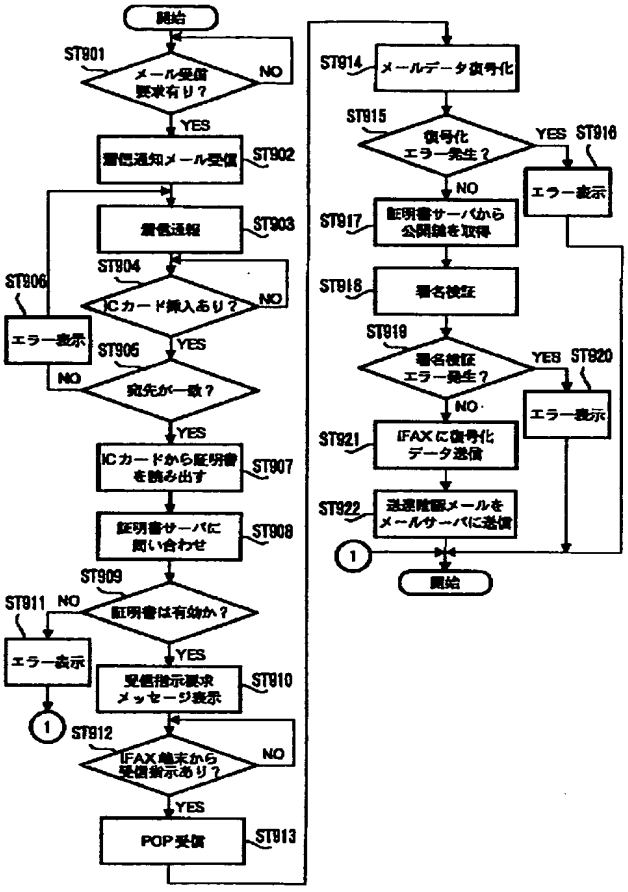
【図８】


開始
宛先指定
ST701
スタートボタン押下
ST702
スキャン
ST703
画像圧縮
ST704
TIFF－F
フォーマットに変換
ST705
セキュアIFAXアダプタに
メッセージ送信
ST706
ST707
セキュア
IFAXアダプタでエラー
あり？
YES
NO
ST709
エラー表示
正常終了表示
ST708
終了

【図９】


開始
ST801
接続要求あり？
NO
YES
ST802
メール受信
ST803
エラー発生あり？
YES
NO
ST804
送信元にエラー
通知メールを
送信
ST805
宛先
アカウントを管理して
いるか？
NO
YES
ST807
メール種別判定
ST806
受信メールを他
のサーバに転送
(SMTP)
ST808
送達確認メールか？
YES
NO
ST813
送信確認メール
を送信元に送信
(SMTP)
ST809
メールボックスに格納
ST810
署名付メールか？
NO
YES
ST811
着信通知メール作成
ST812
着信通知メール送信
(SMTP)
開始

【図１０】



フロントページの続き

(51) Int. Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ（参考）
Ｈ０４Ｎ　1/44		Ｈ０４Ｎ　1/44	

(72)発明者　秋元　正男
東京都目黒区下目黒２丁目３番８号　松下電送システム株式会社内

Ｆターム(参考)　5C062 AA02 AA21 AA29 AA35 AB38 AC38 AF00 BD09
5C075 AB90 CB90 CF04 EE03 EE06
5K030 GA15 HA06 LD13 LD20